PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{7} : H04L 9/00	A1	(11) International Publication Number: **WO 00/57595** (43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/SG99/00020

(22) International Filing Date: 22 March 1999 (22.03.99)

(71) Applicant *(for all designated States except US)*: KENT RIDGE DIGITAL LABS [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BAO, Feng [CN/SG]; 37 West Coast Park, #04–06, Parkview Condo, Singapore 127653 (SG). DENG, Huijie, Robert [SG/SG]; 2 Namly Rise, Singapore 267110 (SG).

(74) Agent: HELEN YEO & PARTNERS; 80 Raffles Place, #33–00 UOB Plaza 1, Singapore 048624 (SG).

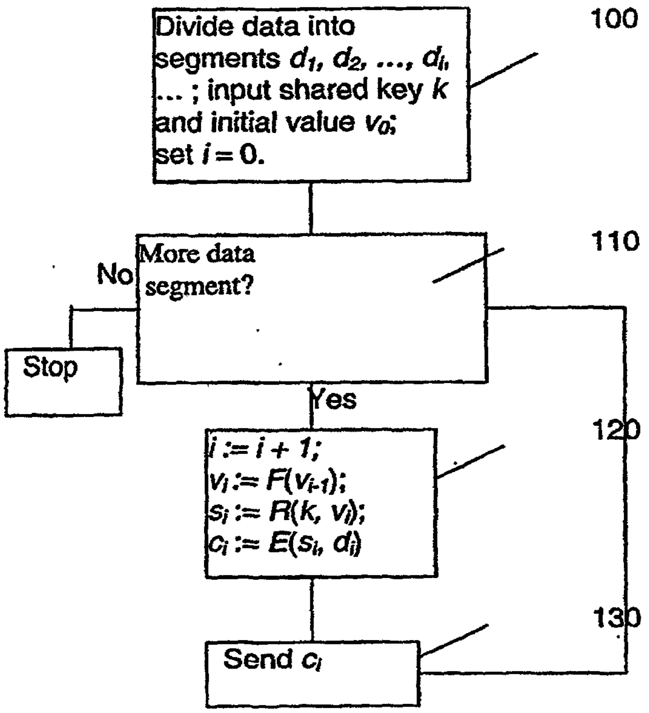
(81) Designated States: JP, SG, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING AND DECRYPTING DATA

(57) Abstract

A method and apparatus for encrypting and decrypting data is disclosed which employs two or more cryptographic algorithms to achieve high throughput without compromizing security. The invention is especially useful for software implementation to protect large amounts of multimedia data over high-speed communication channels.


Divide data into segments $d_1, d_2, \ldots, d_i, \ldots$; input shared key k and initial value v_0; set $i = 0$.
100
More data segment?
110
No
Stop
Yes
$i := i + 1;$
$v_i := F(v_{i-1});$
$s_i := R(k, v_i);$
$c_i := E(s_i, d_i)$
120
Send c_i
130